08-14-00

A

Please type a plus sign (+) inside this box → +

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	042390.P9016
First Inventor or Application Identifier	Ramanathan Ramanathan
Title	METHOD AND APPARATUS FOR MONITORING ENCRYPTED
Express Mail Label No.	EL03443848US

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. ☒ Fee Transmittal Form
(Submit an original, and a duplicate for fee processing)

2. ☒ Specification [*Total Pages 26*]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (*if filed*)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. ☒ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets 6*]

4. Oath or Declaration [*Total Pages 3*]
a. ☒ Newly executed (original copy)
b. ☐ Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 16 completed)
i. ☐ DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR §§ 1.63(d)(2) and 1.33(b).

**NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).*

5. ☐ Microfiche Computer Program *(Appendix)*

6. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. ☐ Computer Readable Copy
b. ☐ Paper Copy (identical to computer copy)
c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. ☒ Assignment Papers (cover sheet & document(s))
8. ☐ 37 C.F.R. § 3.73(b) Statement *(when there is an assignee)* ☐ Power of Attorney
9. ☐ English Translation Document *(if applicable)*
10. ☐ Information Disclosure Statement (IDS)/PTO - 1449 ☐ Copies of IDS Citations
11. ☐ Preliminary Amendment
12. ☒ Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
13. ☐ *Small Entity Statement(s) ☐ Statement filed in prior application, Status still proper and desired
14. ☐ Certified Copy of Priority Document(s)
(if foreign priority is claimed)
15. ☐ Other: .....

16. **If a CONTINUING APPLICATION**, *check appropriate box, and supply the requisite information below and in a preliminary amendment:*
☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No: _____

Prior application Information: Examiner _____ *Group/Art Unit:* _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

☐ *Customer Number or Bar Code Label* *(Insert Customer No. or Attach bar code label here)* *or* ☒ *Correspondence address below*

Name	BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP				
Address	12400 Wilshire Boulevard, Seventh Floor				
City	Los Angeles	*State*	California	*Zip Code*	90025
Country	U.S.A.	*Telephone*	(503) 684-6200	*Fax*	(503) 684-3245

Name (Print/Type)	Clive D. Menezes, Reg. No. 45,493		
Signature		*Date*	08/11/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

JC883 U.S. PTO 08/11/00
JC875 U.S. PTO 09/637123 08/11/00
09637123 081100

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

TITLE OF THE INVENTION

METHOD AND APPARATUS FOR MONITORING ENCRYPTED COMMUNICATIONS IN A NETWORK

INVENTOR

RAMANATHAN RAMANATHAN

042390.P9016

Prepared by

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1026
(503) 684-6200

Express Mail Label No. EL034438484US

COPYRIGHT NOTICE

Contained herein is material that is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction of the patent disclosure by any person as it appears in the Patent and Trademark Office patent files or records, but otherwise reserves all rights to the copyright whatsoever.

BACKGROUND OF THE INVENTION

Field of the Invention

The present invention is related to the field of networking. In particular, the present invention is related to a method and apparatus for monitoring encrypted communications in a network.

Description of the Related Art

Network security is a growing concern of organizations that employ networked computer systems. As a security measure, a corporation may wish to limit the communications between different groups of employees within the organization, or may desire to keep individuals from within the corporate structure from snooping in on the transmission of other employees within the corporation, or the corporation may wish to monitor the content of information that is transmitted between different employees within the corporate network.

key to decrypt the message. Thus, the private keys are not transmitted and are thereby secure. In this method too, a network monitoring element such as a network administrator will be unable to monitor the encrypted communications between two computers on the network as the network monitoring element is not in possession of the key that is needed to decrypt the data. The prior art fails to describe a method or an apparatus for monitoring encrypted communications in a network, by a network administrator or by a network element such as another computer that has the authority to do so.

042390.P9016 Express Mail

BRIEF SUMMARY OF THE DRAWINGS

Figure. 1 illustrates an embodiment of a prior art system wherein data is encrypted.

Figure. 2 illustrates an embodiment of the disclosed invention using a policy server and a policy administrator to monitor encrypted communications in a network.

Figure. 3 is a flow diagram illustrating an overview of an embodiment of the invention.

Figure. 4 is a flow diagram of the communication process between network elements.

Figure. 5 is a flow diagram illustrating details of an embodiment of the invention.

Figure 6. illustrates a policy server comprising an embodiment of the invention.

Figure 7. illustrates a network monitoring element comprising an embodiment of the invention.

042390.P9016

DETAILED DESCRIPTION OF THE INVENTION

Described is a method and apparatus for monitoring encrypted communications in a network. In particular, the invention describes a method and apparatus for monitoring encrypted communications in a network comprising establishing a network policy (NP) on a policy server, establishing a network monitoring digital contract (NMDC) between the policy server and a network monitoring element, establishing a network use digital contract (NUDC) between the policy server and a first network element, establishing a NUDC between the policy server and a second network element, and monitoring communications between the first network element and the second network element, by the network monitoring element, in accordance with the network policy, the network monitoring digital contract, and network use digital contracts.

In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one of ordinary skill in the art that the present invention may be practiced without these specific details. In other instances, well-known architectures, steps, and techniques have not been shown to avoid unnecessarily obscuring the present invention. For example, specific details are not provided as to whether the method is implemented in local area network (LAN), a wide area network (WAN), or across the Internet. Also, specific details are not provided as to whether the method is implemented as a software routine, hardware circuit, firmware, or a combination thereof. While the description that follows addresses the method as it applies to a Local Area Network (LAN) application, it is appreciated by those of ordinary skill in the art that the method is generally applicable

to any network application including, but not limited to, internetworks (Internet), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs).

In one embodiment, Figures 2 and 3 illustrate a network comprising a plurality of policy servers 201, a plurality of network monitoring elements 202, and network elements 203 and 204 (such as computers). At 300, a network policy (NP) is defined, distributed and administered by policy administrator 205. At 310 the policy administrator transmits the NP to each network element. A network element may only communicate with another network element in accordance with a particular communication rule defined in the NP. If two network elements are allowed to communicate with each other, the NP stipulates the type of encryption algorithm, authentication algorithm, the type of keys used for encryption and authentication, and the duration of time during which the keys are valid. The term network element as used here is generic and is to be construed to include any network element including computers, which may communicate with each other.

In 320, once the NP has been transmitted to each network element, a network monitoring element 202 that desires to monitor the communication between network elements 203 and 204, obtains a network monitoring digital contract (NMDC) from the policy administrator 205. Although the description that follows is for a network administrator to monitor communication between network elements, any network element that possesses the required authorization as indicated in the NP may monitor the communications between network elements. In one embodiment the policy administrator 205, and the network monitoring element 202, are physically located on the same device. In one embodiment, prior to issuing the NMDC, the policy administrator 205

authenticates the network administrator 202 by requesting from the network administrator its proof of identity. In one embodiment this proof of identity is a digital certificate. A digital certificate is the digital equivalent of an identity (ID) card used in conjunction with a public key encryption system. Digital certificates are well known in the art and are issued by third parties known as certification authorities (CAs) such as VeriSign, Inc., of Mountain View, CA. After receiving the digital certificate from the network administrator 202 and after authenticating the network administrator, the policy administrator 205 requests and receives from the network administrator 202 the network administrator's authorization, which in one embodiment is a legal corporate authorization. The network administrator's authorization or legal corporate authorization validates the network administrator's authority to monitor network communications as specified in the NP. The authorization, or legal corporate authorization comprises a digital signature. A digital signature is an electronic signature that is well known in the art. The policy administrator authenticates the network administrator's digital signature. On receiving and authenticating both, the digital certificate that authenticates the network administrator, as well as the digital signature that validates the network administrator's authority to monitor network communications, the policy administrator 205 issues the network monitoring element a NMDC. The NMDC includes the digital certificate of the policy administrator 205, the digital certificate of the network administrator 202, the digital signature of the network administrator 202, the digital signature of the policy administrator 205, the date, the time, and the content of the transaction. In one embodiment the content of the transaction includes the type of decrypting information to be transmitted, including the decrypting keys needed for decrypting the encrypted

DOCKET NO. 042390.P9016

communication between the communicating elements. The NMDC also includes the period during which the NMDC is valid. A copy of the NMDC is maintained on the policy administrator 205 prior to transmitting the NMDC to the network administrator 202. On receipt of the NMDC, the network administrator maintains a copy for future use.

The network administrator 202 transmits the NMDC to the policy administrator 205 each time the network administrator desires monitoring the communications between network elements. The policy administrator 205 verifies the validity of the NMDC and issues the network administrator the information it needs to decrypt the communication between the elements it intends to monitor. The aforementioned validation process is performed each time the network administrator desires monitoring the encrypted communications because the decryption keys could be different for each set of communicating elements. The network administrator has to renew its NMDC once the NMDC expires. The process to renew the NMDC is as explained above.

In addition to the NMDC, at 330, a second digital contract called the network use digital contract (NUDC) is established between each network element and the policy administrator 205. In particular, each network element registers itself with the policy administrator 205 as one of the policy server's clients and agrees to be bound by the rules in the NP and the NUDC. The NUDC includes the digital certificate of the registering network element 203, the digital certificate of the policy administrator 205, the digital signature of the policy server, the digital signature of the network element, the date, the time, the content of the transaction, and the period during which the NUDC is valid. In one embodiment a copy of the NUDC is maintained on the policy server and on the network element. The NUDC is valid as long as the network element follows the rules

established by the NP and the NUDC. In one embodiment, if the network element chooses not to follow the established rules, a record of the infraction is maintained in its encryption and authentication log, a copy of the infraction is sent to the policy administrator, and the network element will not be able to communicate with other network elements on the network. In one embodiment, the content of the transaction in the NUDC includes establishing the authority for the policy administrator 205 to secretly access the encryption and authentication log and obtain the decryption information stored on the network element. Establishment of such authority may be performed using any one of a number of authorization techniques known in the art.

Referring to figure 4, after the NP, the NMDC and the NUDC are in place, at 400 a network element 203 desires to communicate with another network element 204, at 410 network element 203 looks up the NP it received from the policy administrator 205 to determine if it has the authority to communicate with network element 204. If the authority to communicate exists, at 420, network element 203 determines whether to communicate with network element 204 using the encryption and authentication rules of the NP or its own encryption and authentication algorithm. At 430, network element 203 having decided to use its own encryption and authentication algorithm, logs the details of the encryption and authentication algorithms including any keys needed to decrypt the communications between network elements 203 and 204. In one embodiment, the logs stored on network element 203 are stored in an encrypted format. At 440, network element 203 after logging the encryption and authentication algorithm it intends using, including the decrypting keys, communicates with network element 204 in an encrypted format. At 450, network element 203 logs the encryption and authentication algorithm

including the decrypting keys as specified by the NP. In one embodiment, the logs stored on the policy server are in an encrypted format. At 460, network element 203 uses the encryption and authenticating algorithm logged and communicates with network element 204.

Referring to figure 5, the process by which network administrator 202 monitors encrypted communications between network elements 203 and 204 will now be described. At 581, the NMDC and the NUDC have been established. At 500, network administrator 202 decides to monitor the communications between network elements 203 and 204. At 510, the policy administrator 205 receives the NMDC from the network administrator 202. At 520, the policy administrator 205 authenticates the NMDC. After determining that the NMDC is valid, at 540 the policy administrator determines whether it has the decrypting information in its own log. In one embodiment, decrypting information includes decrypting keys for decrypting the encrypted communications between the network elements. If the policy administrator has the decrypting information, at 560 the policy administrator transmits the decrypting information to network administrator 202. At 590, the network administrator uses the decrypting information obtained from the policy administrator to decrypt the encrypted communications between network elements 203 and 204. At 550, if policy administrator does not have the decrypting information in its log, it obtains the decrypting information from the log on network elements 203 or 204 and transmits the decrypting information to the network administrator 202. In another embodiment, at 580, policy administrator 202 decrypts the communication between network elements 203 and 204 and transmits the

information to network administrator 202. This transfer of information is done via a secure link between the policy administrator 205 and the network administrator 202.

Figure 6 illustrates an apparatus of an embodiment of the invention. In particular, figure 6 illustrates a policy server in which an embodiment of the invention is employed. The apparatus comprises a receiver 600 to receive an NMDC from a network monitoring element and to receive a request for decrypting communications between network elements. Communicatively coupled to the receiver is a microprocessor 610 with a memory 620. The microprocessor 610 authenticates the NMDC and retrieves decrypting information either from memory 620 or from network elements. Communicatively coupled to the microprocessor 610 is a transmitter 630 for transmitting the initial copy of the NMDC to the network monitoring element, for transmitting a copy of the NUDC to a network element, and for transmitting decrypting information, including decrypting keys that are used by the network monitoring element to decrypt the encrypted communications between network elements. In one embodiment the microprocessor reads the logs containing the decrypting information on a network element, and obtains the decrypting keys, decrypts the communication between network elements and the transmitter transmits the decrypted communications to the network monitoring element.

Figure 7 illustrates an apparatus of an embodiment of the invention. In particular, figure 7 illustrates a network monitoring element in which an embodiment of the invention is employed. The apparatus comprises a receiver 700 to initially receive the NMDC from the policy administrator, and to subsequently receive decrypting information, including decrypting keys to decrypt the encrypted communication it receives between network elements. In one embodiment the receiver 700 receives the